neustar
Real Intelligence. Better Decisions.

Security-Related Information

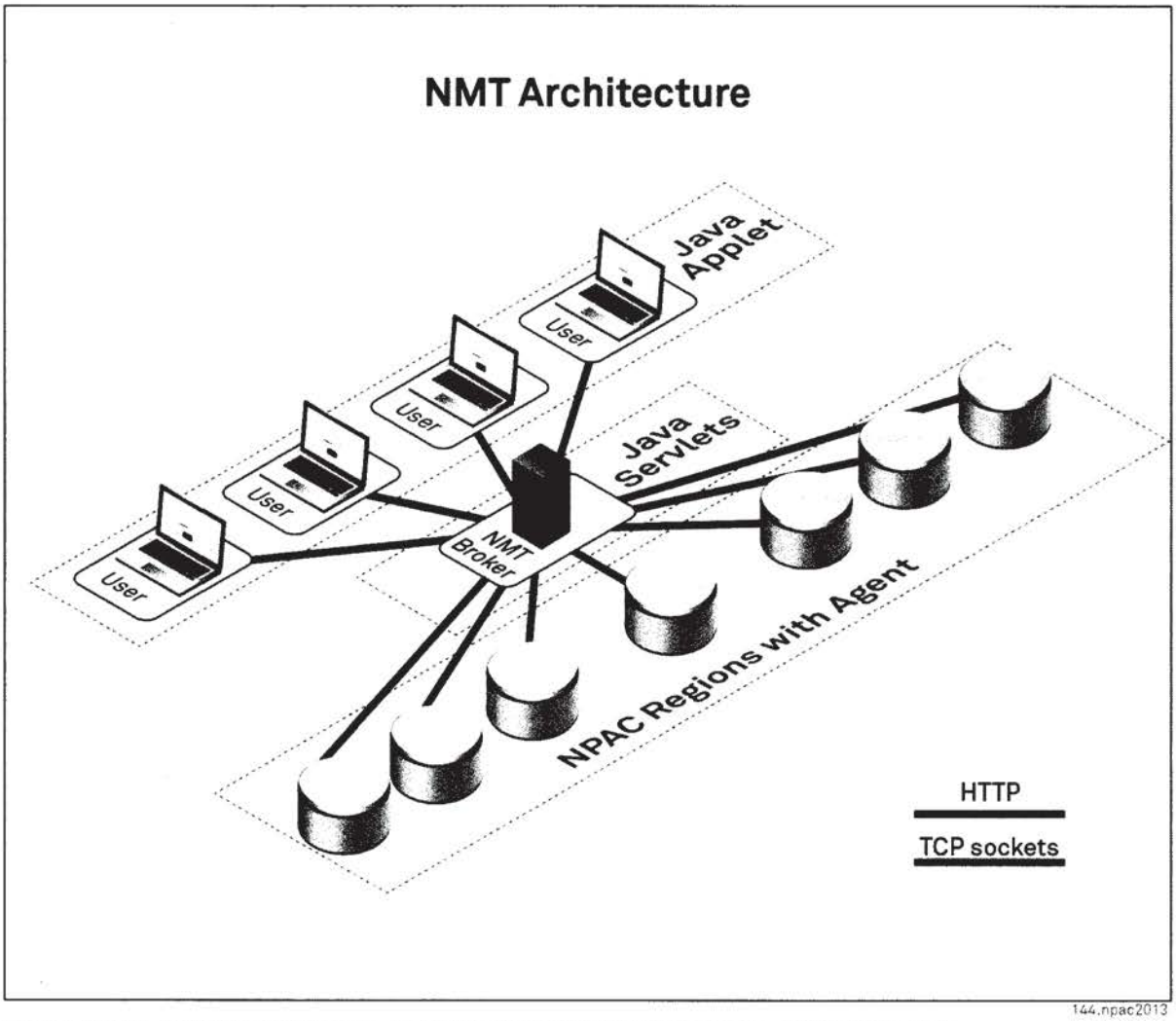

Exhibit 1.2.3-6: NMT provides an overview of all NPAC/SMS service-critical metrics.

As Mass Update Mass Port jobs are executed, the system tracks queues for LSMSs. If these queues rise above configurable thresholds, all jobs are suspended. This prevents failed LSMS broadcasts and ensures all LSMSs are synchronized. The system monitors the success rate of all work within each job. If a job has too many failures, it is paused so it can be reviewed and corrected. With both of these features, NPAC personnel are alerted whenever the system preempts a job.

Neustar has developed an extensive set of queries that analyze the production system for logical inconsistencies and that identify potential problems with Service Provider systems. For example, if an LSMS remains on the failed list of a subscription version for longer than one day then the subscription version is included in a report that is e-mailed to NPAC support personnel for investigation. This allows Neustar to remain in front of issues before they cause actual problems. Analysis of an issue is performed on copies of the production database to prevent interference with online processing.

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Security-Related Information

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

1.3 Neustar's Approach to Operational Excellence

Why Neustar

- Detailed methodology to release management including over 60,000 regression test cases
- Exceptional results from operations; audited by a third-party
- Investment in simulation of actual traffic patterns and characteristics to ensure high-quality software releases

New for the Next Term

- Implementing and certifying in:
  - TL 9000 audit, which is designed for and by the communications Industry
  - ISO 27001 Information Security Standard, which minimizes and defends against security threats in the ever changing ecosystem
  - ISO 22301 Business Continuity Standard, which serves to further strengthen our ability to continue operations when faced with catastrophic events
- QA Testing and Release Management Processes
  - Software security assurance
  - NPAC User Interface load test to assess capacity and plan for future expansion of users
- Continuous integration to improve software code velocity

Operational excellence is often used to describe a company's total quality management (TQM) approach which usually includes at a minimum, measuring key processes, developing metrics and alerts, identifying anomalies or deviations from standard patterns, and driving continual improvement. Neustar's corporate-wide TQM includes those principles as well; however, we believe that most of our success is attributable to the following.

- Corporate and personnel-level **commitment to rigor, continuous improvement, and innovation via the consistent use of and adherence to industry best practices** in project management, software development and testing, change management, and service delivery while being agile enough to meet evolving needs.

- Corporate and personnel-level **commitment to the maintenance and satisfaction of various third-party audits, industry benchmarks, and certifications**.

- **Proactive and holistic approach to performance monitoring and management** of not only the LNPA Service and system but also the LNP ecosystem, including Service Provider's LSMSs and SOAs, that could negatively impact NPAC/SMS performance and drive efficiency out of the system.

- **Leveraging subject matter expertise** and a corporate commitment to continually invest in human capital with training and certifications to ensure employee satisfaction. This expertise should be not only job specific (e.g., software development, security, etc.) but also expertise in Numbering, LNP, the NPAC/SMS, and the ecosystem the NPAC/SMS supports. Neustar's team of experts has been the single most important factor in our success as a vendor for the Industry—not just for LNPA but also for other Industry-wide services like Thousands-block Number Pooling Administration and NANP Administration. Our personnel are active in many forums that seek to develop and implement policies that address the changing needs of the Industry—for example, PSTN to IP migration, IP interconnection etc. We describe our LNP expertise further in Proposal Section 2.4, LNP Expertise.

Each element highlighted above, depicted in Exhibit 1.3-1, and described in further detail below, has enabled us to continually improve over the years to deliver reliable, predictable levels of performance thus allowing Service Providers to focus their resources and attention on revenue-generating objectives rather than expend energy to manage a poorly performing vendor.

1.3.1 Rigor Through Consistent Use of and Adherence to Industry Best Practices

Neustar's Project Management Approach

The old adage rings true: failing to plan is planning to fail, particularly when implementing changes to an Industry-wide infrastructure resource such as the NPAC/SMS where every SP must continue to be able to operate and affect portability seamlessly. Developing and implementing a solid, realistic plan requires both function-specific expertise and experience (e.g., certified project managers) and subject matter expertise and experience (e.g., experience implementing NPAC/SMS changes). Without this, the LNP Administrator cannot develop a plan that adequately addresses the requisite activities/milestones, the resources required, dependencies, or the duration of these activities, including any environment considerations (e.g., Industry needs regarding testing times, documentation requirements, training requirements, etc.). Neustar understands this and has invested in two corporate-wide project management organizations (PMO)—one for NPAC Infrastructure and Operations and one for NPAC Software Development and Testing—which are responsible for overall coordination of every change to the NPAC/SMS from the standard, routine maintenance-type changes up to major software release and technology refresh projects to ensure every change made to the NPAC/SMS is well managed, leverages the appropriate expertise and resources, and is governed by a set of documented, proven project management processes and methodologies.

Exhibit 1.3-1: **Neustar leverages unmatched expertise to take a proactive approach to managing with rigor to deliver predictable and reliable services to the Industry.**

Our PMBOK-based approach to project management for NPAC projects will continue to encompass the management of the following critical components:

- Project schedule
- Staffing
- Project organization
- Monitoring and control

- Risk management
- Project planning and tracking
- Communication
- Issue escalation
- Quality assurance (QA) monitoring

Neustar's Software Development Process

Neustar follows custom ISO 9001:2000 certified processes finely tuned from years of experience managing the NPAC to ensure successful production rollout that does not impact the LNP ecosystem or NPAC/SMS performance. Our NPAC Development team works closely with the NPAC QA and Operations teams from start to finish ensuring all teams are fully aware of the operational implications of the implementations provided by NPAC Development. This collaboration takes the form of joint planning sessions where the teams discuss the proposed feature/change and make joint decisions on high-level requirements, as well as transition meetings held prior to delivery.

> TMNG assesses Neustar's Software Release Management process to be well above what is typically encountered in the industry.
>
> TMNG—2012 Article 14 audit

The following is a high-level outline of the Customized NPAC Software Development and Testing Process and is shown in Exhibit 1.3-2.

Requirements Definition and Statement of Work (SOW)

The NPAC Development process provides input and support to the NPAC SOW Development Process as described below. This phase is iterative in nature and comprises a two-way process. Neustar, as the LNPA, proposes requirements (driven by continuous improvement and refinement objectives) to the Industry and receives and processes feedback:

- **LNPA-WG Change Management**—Neustar's NPAC representatives participate in LNPA WG meetings as NPAC change order requirements are discussed, refined, prioritized, and documented. Our development team reviews and analyzes the requirements to ensure they are clearly defined, technically feasible, and can be implemented within the requested timeframe.
- **NPAC Change Order Analysis and Estimation**—Neustar gathers up technical inputs from various internal teams to draft the SOW. We analyze the NPAC release package to resolve issues, answer questions, verify the scope has not changed, assess impacts to the current NPAC/SMS, prepare level-of-effort estimates, and create draft schedules. This process may occur multiple times until a final, negotiated release package is approved by the NAPM LLC and Neustar.
- **NPAC SOW Change Management**—Neustar's Customer Relations team notifies NPAC Development/QA that the NPAC SOW is approved and development of the new release begins. The negotiated release package, including the approved change orders, is used throughout design and development.

Exhibit 1.3-2: Neustar's unique approach to NPAC SW development enables us to consistently perform over 25 iterations of testing cycles, running over 60,000 test cases, and deliver near-perfect application releases to production.

Software Design, Development, and QA Testing

Our ISO-certified NPAC Software Design and Development Process has been refined and customized over the years to address the NPAC's specific needs. Most importantly, the NPAC Development team and the NPAC QA team are co-located and work hand in hand and concurrently during this phase. Nearly every activity in this phase that the Development team executes is mirrored by the QA team for testing purposes. The numerous benefits of this unique approach are discussed in the Neustar Difference below. This phase of the process includes:

- **Requirements analysis**—Development and QA teams perform a detailed review of the requirements to ensure requirements are understood and determine if development of derived requirements is necessary. This is an iterative process where many of the potential roadblocks are discovered and discussed with customers resulting in clarity. Customer and stakeholder involvement is essential to fine tuning the feature set even at late stages of Neustar Development.

- **System design and detailed design**—NPAC software engineers determine and document the high-level system design and the detailed design to meet the change order requirements.

- Security-Related Information

- **System Functional Testing**—NPAC QA Team runs Automated Functional Tests developed to test the new features in Change Orders.

- Security-Related Information

The Neustar Difference

While there are very strong parallels between Neustar's custom approach to NPAC Software Development and the Agile Manifesto, our approach is customized for the NPAC/SMS and has proven to be very successful. The advantages of this tight integration between our Development and QA teams include:

- The ability to absorb any last minute changes with the sense of confidence that comes with executing Automated Testing—even for the new features in the release—no matter how late these changes are decided. Manual testing cannot achieve this level of confidence due to time pressures.
- Software quality is an evolutionary process where software gets better after each iteration. Using fully automated testing enables many more iterations of internal releases and test cycles than can be achieved by segregated/out-of-synch software teams. Security-Related Information
- The QA/Dev Team's early access to internal builds enables early detection of issues, allowing ample time for reliable fixes. In addition, early access reduces the amount of testing that the QA/Dev Team has to do, allowing us to move faster and focus on more sophisticated development problems.
- Security-Related Information

QA Testing and Release Management

Prior to the Integration Test phase, the NPAC Development Release Control Board (RCB) meets to review the status of NPAC code, decide on which defect fixes and enhancements to include in the release, and determine the most appropriate release type (e.g., major, point, patch). In addition, the NPAC Development Systems Architect prepares Release Notes that describe (for Applications Support) the release contents, any known issues included in the release (if applicable), and installation and back-out instructions as required. 'Known issues' are also documented in the Security-Related Information system for RCB consideration in a future release.

Security-Related Information

Neustar has studied the traffic patterns on Production Regions very closely over the years, and developed Load Generators that simulate predicted production load volumes. This helps with future capacity planning and flawless operations under spikes of volumes, whether it's network maintenance or launch of new phones by a Service Provider.

For the next term, we plan on implementing the following refinements:

new

- Security-Related Information

- **GUI Load Test to assess capacity and plan for future expansion of users**—As more features are made available to SPIDs, the use of NPAC GUI is increasing. We will use Security-Related Information to develop load and performance tests to measure how fast it is expected to perform under real-life transaction volumes and measure the capacity of NPAC UI. By using this, we strengthen our ability to accurately anticipate future capacity needs.

- **Break Testing to assess and improve system's reliability even further**—Developing a set of catastrophe scenarios, for example, killing processes in the middle of transactions, to assess the resilience of the NPAC system. Such testing would tell us potential data/transaction loss during unexpected catastrophic events, so that we prepare even better for such disastrous scenarios.

- **Continuous Integration to improve code velocity**—Implementing a daily task that kicks off the build process automatically, integrating pieces each engineer is working on, and deploy the build on all Dev and QA servers. Continuous Integration allows integrating pieces more often and in smaller chunks so we can resolve integration problems faster. This would be followed by kicking-off a set of Automated Sanity Tests to test the build allowing Development Engineers to make use of Automated Tests during their Integration.

The Neustar Difference

n

During this phase, there are several things that Neustar does that sets us apart from our competitors. These include:

- Security-Related Information

- Meticulous internal acceptance testing. For example, when making a major change that involves data conversion, the NPAC Applications Team receives a copy of the production data and runs through the actual upgrade on each region to make sure we don't encounter data-specific issues that could never be found in the QA environment due to the nature of the data. The added benefit of this exercise is that it gives the NPAC/SMS Application Team the opportunity to rehearse the procedures such that at deployment time they are just repeating steps they have executed successfully already.

The following functions are aligned in support of these phases:

- **Tier 3 Support**—NPAC developers assigned to Tier 3 Support investigate and verify a defect, evaluate the impact severity, open a ticket and maintain information about the problem in ALM, and determine the appropriate course of action. Potential actions include 1) identify a work-around solution and schedule fix for a future point release, 2) build an emergency patch release containing a code fix, and 3) provide an explanation for the system behavior. Tier 3 Support is available 24x7x365.

- **Project Management (PM)**—NPAC Software PMO is responsible for planning, coordinating, and oversight including task estimation, project scheduling, resource management, risk management, project cost and budget tracking, and project close-out. In addition, the NPAC Director, CMA, and NPAC Project Manager plan the manpower, training, hardware, facilities, and other resources needed to complete the project. The project schedule and cost estimates are updated at the end of system design and detailed design to factor in revised work-hour estimates and actual hours worked.

- **Configuration Management (CM)**—The CM Engineer manages the build and release process used for Integration, System, and Patch Release testing. This includes generating builds, installing builds on development boxes, releasing source code and contacting developers to resolve issues when builds fail. The System Architect is responsible for writing release notes, coordinating and conducting release readiness reviews with the assistance of the Project manager, moving approved releases, and supporting release notes to an FTP site for use by Application Support in their verification, validation, and Production implementation. In addition, the System Architect implements and maintains CM standards and procedures, reviews technical product specifications to ensure overall product quality, maintains CM documentation, and creates release packages and release notes. Records of all releases can be found in the Telelogic CM Synergy repository.

Security-Related Information

The Neustar Difference

In conclusion, typical software development programs have testing in place but not every vendor undertakes testing with the same approach and vigor. Security-Related Information

As the current NPAC provider, Neustar has successfully implemented 11 major software releases to the NPAC system, each one in conformance with new requirements, provided on time and within budget, and with Security-Related Information

Exhibit 1.3-3 provides a listing of third-party audits and shows how we have improved over the past years in Software Release Management.

Neustar is ISO 9001:2000 certified for the NPAC system. Detailed region roll-out plans are developed and executed for the implementation of NPAC/SMS software releases in the production NPAC regions. Exhibit 1.3-4 is provided for reference as a sample of a region rollout plan.

Security-Related Information

This may not be intuitive to a less experienced vendor that might not appreciate the consequences of introducing errors. Problems that surface during implementation in production can take on a life of their own and very quickly overwhelm not just the NPAC but the entire ecosystem and can even cause carriers to lose their ability to transact with the NPAC. Security-Related Information

Software Release Management–Article 14 Audit Scores

Category	2008	2012	Trend
Software Release Management Overall Score	**4.50**	**4.66**	▲
Protecting Service Providers Operations	**4.50**	**4.67**	▲
Certification and Regression Testing	4.40	4.67	▲
Interoperability Testing	5.00	5.00	⟷
Software Defect Management	[redacted]		▲
Delivering New Software Releases			
Complete Release Life Cycle	4.50	4.59	▲
Requirements Analysis & System Design	5.00	5.00	⟷
Development	4.10	4.20	▲
Neustar Quality Assurance	5.00	5.00	⟷
Industry Testing Support	4.50	4.60	▲
Production Rollout and Rollback	4.30	4.50	▲
Project Management	4.40	4.40	⟷
Maintaining Release Management Support	**4.30**	**4.36**	▲
Business & System Expertise	4.10	4.20	▲
Trained Staff	4.10	4.20	▲
System Architecture	4.50	4.50	⟷
System Documentation	4.50	4.50	⟷
Infrastructure and Support Tools	4.50	4.50	⟷

5 - Excellent performance, far exceeds industry best practices
4 - Above average performance, generally exceeds industry best practices
3 - Average performance, meets industry best practices
2 - Below average performance, fails to meet industry best practices
1 - Poor performance, falls far below industry best practices

065.npac2013

Exhibit 1.3-3: Third-party audits validate our performance and provide vauable input on possible future enhancements.

Neustar's Internal Change Management Process

Waiting for system components to fail or come to "end of life" is not a responsible strategy for ensuring carrier-grade performance. Once changes are deemed necessary, we follow an ISO-certified, NPAC-customized Change Management process (shown in Exhibit 1.3-5) to virtually eliminate risk and maximize success. The following are highlights of Neustar's approach that we will continue to use in the next term:

- Security-Related Information

- **Neustar Infrastructure & Operations Teams perform proactive maintenance on the NPAC/SMS to ensure optimal performance.** Examples include, database index rebuilds, storage array quarterly health checks, chassis hardware firmware upgrades, hardware server reboots, operating system upgrades, network upgrades, and security firewall upgrades. Security-Related Information

- **Standardized and documented Change Requests are reviewed** and approved by NPAC Product, Customer, and Technical Management teams at a **weekly Change Management Advisory Board Meeting**. Security Relate

- Neustar's Operations Team develops a **Rollout Plan detailing the software application implementation steps and timeline** for implementing NPAC/SMS software application releases in the NPAC Customer Test Environment (CTE) and Production Regions. Neustar performs comprehensive Acceptance and Region Readiness Testing, and coordinates and executes Industry certification Turn-up Testing with Service Providers and their vendors for software application releases prior implementing Production.

The Neustar Difference

Applying lessons learned throughout our tenure, Neustar has refined the CM process to introduce safeguards designed to execute releases and changes more seamlessly to the Industry. Security-Related Information

neustar
Real Intelligence. Better Decisions.

Security-Related Information

Further, we use a customer-mirrored, internal production system for a few weeks prior to deploying to the customer facing production system. Whenever possible, we install the change in just one region for a "burn-in" time of two weeks and actively monitor any new component for anomalies to ensure there are no unwanted side effects or issues internally, or impacts on external systems—SOAs, LSMSs, and NPAC UI users. If there are problems identified, they are addressed quickly, thus minimizing their impact. If the burn-in period has elapsed with no problems, we deploy the change into the remaining regions over several industry-defined maintenance windows. This approach has helped us eliminate virtually all risk to customer systems and NPAC performance.

1.3.2 Rigor Through Third-party Audits, Benchmarks, and Certifications

Audits and Benchmarks are an essential part of Operational Excellence. Neutral independent auditors allow Neustar, the NAPM, NPAC Users, and the FCC to see empirical data that Neustar, as the LNPA, is meeting and/or exceeding all obligations—service delivery, system performance, and contractual. Further, given the evolving nature of these audits, they provide valuable insights with recommendations to enable Neustar to design and implement solutions to improve operations. The following tables (see 1.3-1, 1.3-2 below) highlight the various third-party audits to which we are subject as part of our LNP Administration contract; our record of superior performance under those audits; and the certifications we have in place and are proposing for the next term to ensure we continue to meet the needs of the Industry going forward.

new

In addition to the many yearly audits and benchmarks already performed, we are proposing adding several new audits for the next generation NPAC operations to continue to improve overall operations via the TL 9000 audit (specific to telecom vendors), as well as ISO 27001 "Information Security" and ISO 22301 "Business Continuance" audits.

The Neustar Difference

n

Supporting these audits isn't an exercise of simply checking the box to be contractually compliant. Neustar has found that there is real value in these audits. We also established effective relationships with the Industry representatives based on mutual respect and a commitment to use these audits and findings as a powerful tool to continue to improve the overall service we deliver and the systems and tools we use. This has significantly strengthened our approach and ability to deliver service.

Table 1.3-1. NPAC Audit Overview

Audit / RFP Section	Value
	100% compliance over the last 5 years
Gateway Evaluation Process "GEP" (RFP Section 4.1)	• Focuses the LNPA to deliver excellence in system performance and vital administrative activities. • Validates the LNPA's performance via a neutral third-party auditor. • Foundation block of "Operational Excellence"
[redacted]	

Audit / RFP Section	Value
[redacted]	
NPAC/SMS Data Center Operations Audit (RFP Section 4.4)	**Above Average / Best in Class over the last 5 years** • Validates the LNPA's Data Center operations against industry best practices. • Performed by a neutral, third-party auditor. • Ensures the LNPA's Data Center operations continually keep up with evolving standards. • Foundation block of "Operational Excellence"
[redacted]	
New User Evaluator (NUE) Process (RFP Section 5.1)	**100% compliance since inception in 2009** • Neutral, third-party auditor reviews every use of User Data by Neustar's User Services, all other providers of telecommunications-related services are reviewed only for their initial proposed use of User Data. • Neutral, third-party auditor determines whether access to NPAC is necessary and intended use is a Permitted Use. • Neutral, third-party auditor ensures Neustar, in its activities as a User, is not advantaged because it is also the LNPA
[redacted]	
LNP Enhanced Analytical Platform for Law Enforcement Agencies and Public Safety Answering Point Providers (RFP section 11.2)	**100% compliance since inception in 2006** • Neutral, third-party auditors conduct neutrality, performance, and cost reviews.